



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,027	11/02/2001	Bharat Mediratta	FUSN1-01301US1	1204
28554 7590 10/30/2007 VIERRA MAGEN MARCUS & DENIRO LLP 575 MARKET STREET SUITE 2500 SAN FRANCISCO, CA 94105			EXAMINER ZIA, SYED	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 10/30/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mn

<b>Office Action Summary</b>	<b>Application No.</b> 10/003,027	<b>Applicant(s)</b> MEDIRATTA ET AL.	
	<b>Examiner</b> Syed Zia	<b>Art Unit</b> 2131	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 August 2007.  
 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.  
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-57 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
 6) ☒ Claim(s) 1-57 is/are rejected.  
 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \* c) ☐ None of:  
         1. ☐ Certified copies of the priority documents have been received.  
         2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
     \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

This office action is in response to amendment filed on August 20, 2007. Original application contains claim 1-57. Applicant currently amended claims 1, 3, 7, 11, 13, 16-18, 31, 34, 36-37, 40-41, 49-51, 54, and 57. The amendment filed on August 20, 2007 have been entered and made of record. Therefore, presently Claims 1-57 are pending for further consideration.

### **Response to Arguments**

Applicant's arguments filed August 20, 2007 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-20 applicants argued that the Nguyen (U. S. Patent 5,689,566) does not teach “*automatically determining that said current security scheme is to be replace at any point during logon procedure*”.

This is not found persuasive. Cited prior art teaches system and method for bidirectional security system for computer network, that allows user to select security level, and performs data transfers between network nodes using separate queues.

The system includes at least one client with a client communication device communicating with at least one server. A packet reception device receives transmitted packet data from the server. A first packet is generated and transmitted to the server, with at least part of the first packet having a first packet header containing client identifying information and at

Art Unit: 2131

least part of the client identifying information is encrypted prior to transmission. At least part of the client authenticating information in a second packet header is decrypted and it is determined if the second packet is from the server. The client can terminate the communication if the second packet is from an invalid server. A third packet is generated and transmitted to the server, with at least part of the third packet having a third packet header containing session information. At least part of the session information in the third packet header is encrypted prior to transmission. The server has a communication device for communication with the client and a packet reception device. The client identifying information in the first packet header is decrypted and it is determined if the first packet is from a valid client. The communication is terminated if the first packet is from an invalid client. A second packet is generated and transmitted to the client in response to the first and contains client authenticating information in its header. Thus allows user to select security level (Fig.1-2, col.3 line 33 to col.4 line 40. and col.5 line 33 to line 65, col.8 line 52 to col.9 line 28)).

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims. Accordingly, rejections for Claims 1-57 are respectfully maintained.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Nguyen (U. S. Patent 5,689,566)

Regarding Claim 1 Nguyen teaches a computer implemented method for updating a Current security scheme on a computer system, said computer implemented method comprising the steps of: (a) receiving log-in data for a client during a first log-in attempt; (b) authenticating said client, wherein said step (b) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first result, and (2) employing said first result in determining whether to authenticate said client during said first log-in attempt; (c) completing said first log-in attempt; (d) automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client; and (e) modifying at least one record in said computer system in response to said step (d) before said next log-in attempt, wherein said step

Art Unit: 2131

(e) includes the step of: (1) applying a second function to said value received in said step (a) to obtain a second result (Fig.1-2, col.3 line 33 to col.4 line 40).

Regarding Claim 18 Nguyen teaches a computer implemented method for providing a client with access to a primary system through an intermediate system, said computer implemented method comprising the steps of: (a) creating a log-in record at said intermediate system, wherein said log-in record includes a security identifier and a first encrypted value, wherein said security identifier corresponds to a current security scheme employed by said intermediate system; (b) receiving log-in data for said client; (c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record; (d) obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said first encrypted value at said intermediate system; (e) determining that said current security scheme is to be replaced by a desired security scheme; and (f) modifying said log-in record, wherein said step (f) includes the steps of: (1) updating said security identifier to correspond to said desired security scheme, (2) employing data in said log-in data received in said step (b) to calculate a second encrypted value, and (3) replacing said first encrypted value with said second encrypted value (Fig.1-2, col.3 line 33 to col.4 line 40. and col.5 line 33 to line 65).

Regarding Claim 31 Nguyen teaches a processor readable storage medium having processor readable code embodied on said processor readable storage medium, said processor readable code for programming a processor to perform a method for updating a current security

Art Unit: 2131

scheme on a computer system, said method comprising the steps of: (a) receiving log-in data for a client during a first log-in attempt; (b) authenticating said client, wherein said step (b) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first result, and (2) employing said first result in determining whether to authenticate said client during said first log-in attempt; (c) completing said first log-in attempt; (d) automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client; and (e) modifying at least one record in said computer system in response to said step (d) before said next log-in attempt, wherein said step (e) includes the step of: (1) applying a second function to said value received in said step (a) to obtain a second result (Fig.1-2, col.3 line 33 to col.4 line 40. and col.5 line 33 to line 65).

Regarding Claim 41 Nguyen teaches a processor readable storage medium having processor readable code embodied on said processor readable storage medium, said processor readable code for programming a processor to perform a method for providing a client with access to a primary system through an intermediate system, said method comprising the steps of: (a) creating a log-in record at said intermediate system, wherein said log-in record includes a security identifier and a first encrypted value, wherein said security identifier corresponds to a current security scheme employed by said intermediate system; (b) receiving log-in data for said client; (c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record; (d) obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said

Art Unit: 2131

first encrypted value at said intermediate system; (e) determining that said current security scheme is to be replaced by a desired security scheme; and (f) modifying said log-in record, wherein said step (f) includes the steps of: (1) updating said security identifier to correspond to said desired security scheme, (2) employing data in said log-in data received in said step (b) to calculate a second encrypted value, and (3) replacing said first encrypted value with said second encrypted value (Fig.1-2, col.3 line 33 to col.4 line 40. and col.5 line 33 to line 65).

Regarding Claim 49 Nguyen teaches an apparatus providing a client with access to a primary system through an intermediate system, said apparatus comprising: a processor; and a processor readable storage medium, in communication with said processor, said processor readable storage medium storing code for programming said processor to perform a method for updating a current security scheme on a computer system, wherein said method includes the steps of: (a) receiving log-in data for a client during a first log-in attempt; (b) authenticating said client, wherein said step (b) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first result, and (2) employing said first result in determining whether to authenticate said client during said first log-in attempt; (c) completing said first log-in attempt; (d) automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client; and (e) modifying at least one record in said computer system in response to said step (d), wherein said step (e) includes the step of: (1) applying a second function to said value received in said step (a) to obtain a second result (Fig.1-



Art Unit: 2131

2, col.3 line 33 to col.4 line 40. and col.5 line 33 to line 65).

2. Claims 2-17, 19-30, 32-40, 42-48, and 50-57 are rejected applied as above rejecting claims 1, 18, 31, 41, and 49. Furthermore, Nguyen teaches and describes:

As per Claim 2, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record (col.3 line 55 to line 57).

As per Claim 3, wherein said step (e) includes the step of: (2) replacing said first value in said log-in record with said second result obtained in said step (e)(1) (col.3 line 55 to col.4 line 17).

As per Claim 4, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3line 63 to col.4 line 18).

As per Claim 5, said step (b) includes the steps of: (3) applying a third function to said value in said log-in data to obtain a first credential; and (4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first credential (col.4 line 5 to line 30).

As per Claim 6, wherein said step (b) further includes the step of: (5) forwarding said decrypted

Art Unit: 2131

value to a primary computer system credential (col.4 line 5 to line 30).

As per Claim 7, wherein said step (e) includes the steps of: (2) replacing said first value in said log-in record with said second result obtained in said step (e)(1); (3) applying a fourth function to said value in said log-in record to obtain a second credential; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second credential; and (5) replacing said third value in said log-in record with said fourth value (col. 4 line 41 to col.5 line 33).

As per Claim 8, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3 line 63 to col.4 line 30).

As per Claim 9, wherein said step (b) includes the steps of: (3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and (4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key (col.4 line 41 to line 50).

As per Claim 10, wherein said step (b) further includes the step of: (5) forwarding said decrypted value to a primary computer system (col.4 line 41 to line 65).

As per Claim 11, wherein said step (e) includes the steps of: (2) replacing said first value in said

Art Unit: 2131

log-in record with said second result obtained in said step (e)(1); (3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second encryption key; and (5) replacing said third value in said log-in record with said fourth value (col.4 line 41 to col.5 line 33).

As per Claim 12, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) decrypting a first value in said log-in record to obtain a decrypted value, wherein said step (b)(2)(i) employs said first result as a decryption key; and (ii) forwarding said decrypted value to a primary computer system (col.4 line 50 to line 65).

As per Claim 13, wherein said step (d) includes the steps of: (2) encrypting a quantity to obtain a second value, wherein said step (e)(3) employs said second result obtained in said step (e)(1); and (3) replacing said first value in said log-in record with said second value (col.5 line 7 to line 33).

As per Claim 14, wherein: said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3line 63 to col.4 line 18).

As per Claim 15, wherein: said first function is a first cryptographic cipher and said second

Art Unit: 2131

function is a second cryptographic cipher different than said first cryptographic cipher, and said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher (col.3 line 63 to col.4 line 40).

As per Claim 16, further including the steps of: (f) receiving log-in data for said client during a second log-in attempt; (g) authenticating said client during said second log-in attempt, wherein said step (g) includes the steps of: (1) applying said second function to a value in said log-in data received in said step (f) to obtain a third result, and (2) employing said third result in determining whether to authenticate said client during said second log-in attempt (col.3 line 40 to col.4 line 65).

As per Claim 17, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said computer implemented method further including the step of: (h) replacing said first entry in said log-in record with a second entry identifying said desired security scheme (col.8 line 52 to col.9 line 28).

As per Claim 19, wherein said step (c) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first result, and (2) comparing said first result obtained in said step (c)(1) to a first value stored in said log-in record (col.3 line 55 to line 57).

As per Claim 20, wherein said step (f) includes the steps of: (4) applying a second function to

Art Unit: 2131

said value in said log-in data to obtain a second result; and (5) replacing said first value in said log-in record with said second result obtained in said step (d)(4) (col.3 line 55 to col.4 line 17).

As per Claim 21, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3line 63 to col.4 line 18).

As per Claim 22, wherein said step (d) includes the steps of: (3) applying a third function to said value in said log-in data to obtain a first credential; and (4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first credential, wherein said authentication data includes said first decrypted value credential (col.4 line 5 to line 30).

As per Claim 23, said step (f)(2) includes the steps of: (i) applying a fourth function to said value in said log-in record to obtain a second credential; and (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential (col. 4 line 41 to col.5 line 33).

As per Claim 24, said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3 line 63 to col.4 line 30).

As per Claim 25, wherein said step (d) includes the steps of: (3) inputting said value in said log-in data to a first cryptographic cipher to obtain a first decryption key; and (4) decrypting said

Art Unit: 2131

first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first decryption key, wherein said authentication data includes said first decrypted value (col. 4 line 41 to line 50).

As per Claim 26, wherein said step (f)(2) includes the steps of: (i) inputting said value in said log-in record to a second cryptographic cipher to obtain said second encryption key; (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second encryption key (col.5 line 7 to line 33).

As per Claim 27, wherein said step (d) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first credential; and (2) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(2) employs said first credential, wherein said authentication data includes said first decrypted value credential (col.4 line 5 to line 30).

As per Claim 28, wherein said step (f)(2) includes the steps of: (i) applying a second function to said value in said log-in record to obtain a second credential; and (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential (col.4 line 41 to lcol.5 line 33).

As per Claim 29, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3line 63 to col.4 line 18)..

Art Unit: 2131

As per Claim 30, wherein said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher (col.3line 63 to col.4 line 18).

As per Claim 32, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record, and wherein said step (e) includes the step of: (2) replacing said first value in said log-in record with said second result obtained in said step (d)(1) (col. 4 line 41 to col.5 line 65).

As per Claim 33, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3line 63 to col.4 line 18).

As per Claim 34, wherein said step (b) includes the steps of: (3) applying a third function to said value in said log-in data to obtain a first credential; and (4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first credential, and wherein said step (e) includes the steps of: (3) applying a fourth function to said value in said log-in record to obtain a second credential; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second credential; and (5) replacing said third value in said log-in record with said fourth value (col. 4 line 41 to col.5 line 65).

Art Unit: 2131

As per Claim 35, wherein: said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function(col.3 line 63 to col.4 line 30).

As per Claim 36, wherein said step (b) includes the steps of: (3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and (4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key, and wherein said step (e) includes the steps of: (3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second encryption key; and (5) replacing said third value in said log-in record with said fourth value(col.4 line 41 to col.5 line 65).

As per Claim 37, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) decrypting a first value in said log-in record to obtain a decrypted value, wherein said step (b)(2)(i) employs said first result as a decryption key; and (ii) forwarding said decrypted value to a primary computer system, and wherein said step (d) includes the steps of: (2) encrypting a quantity to obtain a second value, wherein said step (e)(2) employs said second result obtained in said step (e)(1); and (3) replacing said first value in said log-in record with said second value (col.4 line 41 to col.5 line 65).



Art Unit: 2131

As per Claim 38, wherein: said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3line 63 to col.4 line 18).

As per Claim 39, wherein: said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher, and said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher (col.3line 63 to col.4 line 18).

As per Claim 40, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said computer implemented method further including the step of: (f) replacing said first entry in said log-in record with a second entry identifying said desired security scheme (col.3 line 33 to col.4 line 40).

As per Claim 42, wherein said step (c) includes the steps of: (1) applying a first function to a value in said log-in data to obtain a first result, and (2) comparing said first result obtained in said step (c)(1) to a first value stored in said log-in record, and wherein said step (f) includes the steps of: (4) applying a second function to said value in said log-in data to obtain a second result; and (5) replacing said first value in said log-in record with said second result obtained in said step (d)(4) (col.4 line 41 to col.5 line 65).

Art Unit: 2131

As per Claim 43, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3 line 55 to col.4 line 17).

As per Claim 44, wherein said step (d) includes the steps of: (3) applying a third function to said value in said log-in data to obtain a first credential; and (4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first credential, wherein said authentication data includes said first decrypted value, and wherein said step (f)(2) includes the steps of: (i) applying a fourth function to said value in said log-in record to obtain a second credential; and (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential (col.4 line 41 to col.5 line 65).

As per Claim 45, wherein said step (d) includes the steps of: (3) inputting said value in said log-in data to a first cryptographic cipher to obtain a first decryption key; and (4) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(4) employs said first decryption key, wherein said authentication data includes said first decrypted value, and wherein said step (f)(2) includes the steps of: (i) inputting said value in said log-in record to a second cryptographic cipher to obtain said second encryption key; (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second encryption key (col.4 line 41 to col.5 line 65).

As per Claim 46, wherein said step (d) includes the steps of: (1) applying a first function to a

Art Unit: 2131

value in said log-in data to obtain a first credential; and (2) decrypting said first encrypted value in said log-in record to obtain a first decrypted value, wherein said step (d)(2) employs said first credential, wherein said authentication data includes said first decrypted value, and wherein said step (f)(2) includes the steps of: (i) applying a second function to said value in said log-in record to obtain a second credential; and (ii) encrypting a quantity to obtain said second encrypted value, wherein said step (f)(2)(ii) employs said second credential (col.4 line 41 to col.5 line 65).

As per Claim 47, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function (col.3line 63 to col.4 line 18).

As per Claim 48, wherein said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher (col.4 line 41 to col.5 line 65).

As per Claim 50, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) comparing said first result obtained in said step (b)(1) to a first value stored in said log-in record, and wherein said step (e) includes the step of: (2) replacing said first value in said log-in record with said second result obtained in said step (e)(1) (col.4 line 41 to col.5 line 65).

As per Claim 51, wherein said step (b) includes the steps of: (3) applying a third function to said value in said log-in data to obtain a first credential; and (4) decrypting a third value in said log-in

Art Unit: 2131

record to obtain a decrypted value, wherein said step (b)(4) employs said first credential, and wherein said step (e) includes the steps of: (3) applying a fourth function to said value in said log-in record to obtain a second credential; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second credential; and (5) replacing said third value in said log-in record with said fourth value (col.4 line 41 to col.5 line 65).

As per Claim 52, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3line 63 to col.4 line 18).

As per Claim 53, wherein said step (b) includes the steps of: (3) inputting said value in said log-in data into a first cryptographic cipher to obtain a first encryption key; and (4) decrypting a third value in said log-in record to obtain a decrypted value, wherein said step (b)(4) employs said first encryption key, wherein said step (e) includes the steps of: (3) inputting said value in said log-in data into a second cryptographic cipher to obtain a second encryption key; (4) encrypting a quantity to obtain a fourth value, wherein said step (e)(4) employs said second encryption key; and (5) replacing said third value in said log-in record with said fourth value (col.4 line 41 to col.5 line 65).

As per Claim 54, wherein said computer system maintains a log-in record, wherein said step (b)(2) includes the steps of: (i) decrypting a first value in said log-in record to obtain a decrypted

Art Unit: 2131

value, wherein said step (b)(2)(i) employs said first result as a decryption key; and (ii) forwarding said decrypted value to a primary computer system, and wherein said step (e) includes the steps of: (2) encrypting a quantity to obtain a second value, wherein said step (e)(2) employs said second result obtained in said step (e)(1); and (3) replacing said first value in said log-in record with said second value (col.4 line 41 to col.5 line 65).

As per Claim 55, wherein said first function is a first hash function and said second function is a second hash function different than said first hash function, and said third function is a third hash function and said fourth function is a fourth hash function different than said third hash function (col.3line 63 to col.4 line 18, and col.5 line 35 to col.5 line 65).

As per Claim 56, wherein said first function is a first cryptographic cipher and said second function is a second cryptographic cipher different than said first cryptographic cipher, and said third function is a third cryptographic cipher and said fourth function is a fourth cryptographic cipher different than said third cryptographic cipher (col.3line 63 to col.4 line 18, and col.5 line 35 to col.5 line 65).

As per Claim 57, wherein said computer system includes a log-in record corresponding to said client, wherein said log-in record includes a first entry identifying said current security scheme, said method further including the step of: (f) replacing said first entry in said log-in record with a second entry identifying said desired security scheme.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SZ

October 20, 2007

  
SYED A. ZIA  
PRIMARY EXAMINER